STANDARD PROCEDURE		PAGE: 1 OF 4	
ISSUED BY:	SECURITY		
EFFECTIVE DATE: 9/29/08			
PROCEDURE #	5.2		
SUBJECT: USERID AND PASSWORDS			
DISTRIBUTION CODE:	A, B, D	CONTACT:	DOR Security Office
		Station:	25
		Phone:	564-5200

I. INTRODUCTION

To comply with the statutory requirements of KRS 131.190 and the Internal Revenue Code (IRC) section 6103, the Kentucky Department of Revenue (DOR) requires that employees shall not intentionally and without authorization inspect or disclose confidential tax information and payroll and personnel information. It is also the policy of the DOR that employees shall obtain written authorization before accessing electronic information. The DOR Security Office shall issue a unique User Identification Number (Userid) to each employee. The Userid is used to grant access to specific computer systems to an employee. The DOR Security Office shall also assign each employee a unique password that the employee must change during his-her first login. In addition to the automatically scheduled expiration and resetting of a password, the employee or the DOR Security Office may change a password whenever there is a need.

II. DEFINITION

For the purpose of this policy, a DOR "employee" is defined to include all recipients of a DOR Userid, such as DOR employees, Internal Revenue Service (IRS) employees, contractors, consultants, Property Valuation Administrators (PVA) and staff, or agents of the PVA and the DOR.

III. POLICY

It is the policy of the DOR that all employees' passwords are confidential and shall be treated as such. The DOR employees shall be made aware of their responsibilities before obtaining access to DOR computers and date to perform their duties.

IV. PROCEDURE

A. Employee Responsibilities

A DOR employee processing or accessing confidential taxpayer data or sensitive administrative information (i.e., personnel, purchasing, and accounting data) within the DOR **must** follow the guidelines outlined in this Standard Procedure.

1. Choose passwords that cannot be easily guessed.

2. Use reasonable efforts to keep passwords confidential.

3. Change password(s) and notify the DOR Security Office immediately, if you suspect that your password(s) has been divulged.

4. Do not, under any circumstance, give anyone your password(s). If anyone, including your supervisor, asks you to divulge your password(s), immediately contact the DOR Security Office. You have ultimate responsibility for any misuse of your password(s).

5. Keep confidential all information that you access through the DOR computer network. All data accessed should be considered sensitive and confidential, unless otherwise specified.

6. Obtain your immediate supervisor's approval before you attempt to operate any DOR computerized systems or access computerized information.

B. Revoking Userid and Resetting Passwords

A password is set to automatically expire after 30 days and the user must enter a new password. However, DOR employees may change their passwords at any time. Instructions for changing passwords are available in the DOR Security Office, if assistance is required.

1. The system will revoke or disable a user's access after three (3) consecutive unsuccessful attempts are made to enter a password. The user must then contact the DOR Security Office to have the password reinstated. If the user does not know his/her password, the DOR Security Office will issue a temporary password that must be changed at the first logon.

2. The employee's immediate supervisor must approve and submit or fax an Authorization to Provide New Password form (13. Forms - 5.2/a) to the DOR Security Office, **within five (5) working days** after a temporary password has been issued. The DOR Security Office will revoke the employee's password if the immediate supervisor fails to submit the Authorization to Provide New Password form within five (5) working days. If the immediate supervisor is not available during the five (5) working days, the employee should obtain approval from their second-line supervisor or another authorized manager in the division. A resumed password does not require the Authorization to Provide New Password form.

3. The employee should choose a new password that has not been previously used.

4. The mainframe system will revoke an employee's Userid if it has not been used within 60 consecutive days. The user must then contact the DOR Security Office to have the Userid resumed. If the user knows his/her current password, the Userid can be resumed. If the user does not know his/her password, the Userid will be enabled by changing the user's assigned password to a temporary password that must be changed at the first logon. An Authorization to Provide New Password form must be completed by the user's immediate supervisor and submitted to the DOR Security Office within five (5) working days. If the immediate supervisor is not available during the five (5) ~~2~~working days, the employee should obtain approval from their second-line supervisor or another authorized manager in the division.

5. When an immediate supervisor revokes an employee's Userid while on an extended leave of absence, the supervisor shall authorize DOR Security Office to enable the Userid when the employee returns to work (KRC Standard Procedure, 5.4, Access to Facilities and Data While On Extended Leave). The supervisor must submit a completed and approved Authorization to Access Department of Revenue Confidential Computer Information form to the DOR Security Office with the relative "start date." If the user knows his/her current password, the Userid can be resumed. If the user does not know his/her password, the DOR Security Office will enable the Userid by changing the user's assigned password to a temporary password that must be changed at the first logon.

C. Password Construction Guidelines

A DOR employee must immediately change his/her password if it has been disclosed to anyone or if they think it has been disclosed. The user shall immediately report the occurrence to the DOR Security Office. The DOR Security Office staff will instruct the user on how to change their password, if assistance is needed.
The password construction guidelines are as follows:

1. Mainframe passwords must be exactly eight (8) alphanumeric characters. Do not use spaces. The only special characters allowed in a mainframe password are the @, # and $.

2. Employee network passwords shall be a minimum of 8 characters.

3. Passwords shall not be stored in batch job control language (JCL).

V. CONFIDENTIAL AND OTHER INFORMATION NOT TO BE DISCLOSED

Employees must maintain the confidentiality of the following types of information:

1. Confidential taxpayer information (KRS 131.190). See 6.1.2 DOR Confidentiality of State and Federal Information.

2. Any other information handles or in the possession of the DOR that is determined to be of a sensitive nature, and which employees are advised.

VI. DISCIPLINARY ACTION

DOR employees are responsible for any misuse of their personal passwords. If a violation of this policy occurs, employees may be subject to disciplinary action, including reprimand, fine and dismissal.

NO STANDARD PROCEDURE MAY BE REVISED BY ADDENDUM, MEMORANDUM OR ANY OTHER MEANS OTHER THAN THOSE SET OUT IN STANDARD PROCEDURE # 1.1 ENTITLED "DOR STANDARD PROCEDURES AND MANUAL."

DISTRIBUTION CODES:

A. Senior Management	**B. Division Directors**	**C. Branch Managers/Supervisors**
D. Cabinet Personnel	**E. Division Personnel**	**F. Branch Personnel**